Remarks/Arguments

In the Final Office Action dated June 18, 2009, it is noted that claims 1 and 3-14 are pending in this application and that claims 1 and 3-14 stand rejected under 35 U.S.C. §103.

Claim 1 has been amended to clarify an aspect of the present invention. This amendment is supported at least by claim 8. Claim 7 has been amended as shown in the listing above to make an editorial change thereto. Claim 2 was cancelled earlier in the prosecution. No new matter has been added.

Cited Art

The following references have been cited and applied in the present Office Action: U.S. Patent 6,526,506 to Lewis (hereinafter referenced as "*Lewis*"); U.S. Patent Application Publication No. 2004/0081320 to Jordan et al. (hereinafter referenced as "*Jordan*"); U.S. Patent 7,293,289 to Loc et al. (hereinafter referenced as "*Loc*"); and U.S. Patent 6,118,869 to Kelem et al. (hereinafter referenced as "*Kelem*").

Rejection of Claims 1, 7-8 and 13 under 35 U.S.C. §103

Claims 1, 7-8 and 13 stand rejected under 35 U.S.C. §103 as being unpatentable over Lewis in view of Jordan. This rejection is respectfully traversed.

Claims 1 and 8 are independent claims. Claim 1 is a method claim, whereas claim 8 is an apparatus claim. Each of claims 1 and 8 recites substantially similar limitations which will be discussed below. It will be understood that, for the sake of brevity of this response, the remarks below are intended to pertain to all the independent claims that include such similar limitations.

Contrary to the assertion in the present Office Action, Lewis fails to teach, show, or suggest "generating a new encryption key at the access point," as defined in claim 1. In the present Office Action at pages 3 and 4, it has been alleged that the definition of "to generate" is "to bring into existence." Then, the same portion of the Office Action concludes that the access point in Lewis brings the new ENCRYPT key into existence. Such a result strays far from the very definition proposed in the Office Action. Moreover, it ignores the teachings of Lewis itself.

When something is brought into existence, it must not have yet existed. Once it exists, it cannot be said to then be brought into existence by some other operation. In Lewis, the key

distribution server generates the new ENCRYPT key. This operation by the key distribution server brings the new ENCRYPT key into existence. Once the new ENCRYPT key exists – that is, once the new ENCRYPT key is generated – it is distributed to the AP. The new ENCRYPT key may then be present on the access point at this time, but there is no operation by the access point that brought the key into existence. The new ENCRYPT key was brought into existence by, and therefore generated on, the key distribution server.

The teachings of Lewis clearly support the fact that only the key distribution server generates, and brings into existence, the new ENCRYPT key. Lewis states quite clearly that the key distribution server 76 includes encryption key generator 150. Lewis then clearly states that "*encryption key generator 150 periodically generates a new ENCRYPT key which is provided to access points 54*" (Lewis at col. 9, lines 42-45). Furthermore, in connection with FIG. 8, Lewis teaches that "*[t]he key distribution server 76 also transmits an update of the current ENCRYPT key which is to be utilized by the respective access points 54. The access points 54 are configured to receive the updated ENCRYPT key and to inform the mobile terminals 66 registered thereto*" (Lewis at col. 14, lines 10-14). This teaching by Lewis cannot be ignored. Moreover, when Lewis describes the functionality of the access points and their encryption/decryption capability, there is not even a remote hint at having the key generation capability of the key distribution server in any of the access points.

For all these reasons, it is believed that Lewis fails to teach, show, or suggest "generating a new encryption key at the access point," as defined in claim 1.

Contrary to the assertion in the present Office Action, Lewis fails to teach, show, or suggest "setting a current encryption key and an old encryption key at an access point in the wireless network," as defined in claim 1. In Lewis, the access point maintains the most current encryption key being used by the mobile terminal, and when the encryption key is changed, the newest encryption key is distributed by the key distribution server 76 to the access point (e.g., Lewis at col. 14, lines 10-14 and FIG. 8; col. 8, lines 16-23 and FIG. 2). As taught by Lewis, the access point is configured to receive the new key from the server 76. However, there is no teaching that the access point has any capability to set both the current and or prior encryption keys. For all these reasons, it is believed that Lewis fails to teach, show, or suggest "setting a current encryption key and an old encryption key at an access point in the wireless network," as defined in claim 1 and similarly in claim 8.

Jordan has been combined with Lewis because it was stated (page 8, Office Action) that Lewis did "not specifically disclose resetting the old encryption key to equal an encryption key being used by a station in communication with the access point" and "wherein a data frame that failed to decrypt using the current encryption key is decrypted using the old encryption key." But Jordan does not cure the deficiencies of Lewis.

Jordan makes no mention of access points or any element that is analogous to an access point. As a result, Jordan cannot be interpreted as disclosing or suggesting generation of encryption keys at access points. Jordan's key generation by password generator 105 is similar to the key generation in Lewis in that it is not performed by an element that even remotely resembles an access point as defined in Applicants' claims. Therefore, Lewis in combination with Jordan fails to disclose or suggest generating encryption keys at an access point.

Jordan, without a device that even resembles an access point, lacks any teaching, showing, or suggestion for "setting a current encryption key and an old encryption key at an access point in the wireless network', of for "generating a new encryption key at the access point," or for "indicating a decryption failure for a data frame received from the station when the encryption key used by the station does not match the current encryption key, wherein a data frame that failed to decrypt using the current encryption key is decrypted by said access point using the old encryption key," all as defined in claim 1 and at least the first and last limitations similarly defined in claim 8. For all these reasons, it is believed that the combination of Lewis and Jordan fails to teach, show, or suggest all the limitations defined in claim 1 and claim 8.

In light of all the remarks above, it is submitted that the limitations of independent claims 1 and 8 and the claims dependent thereon would not have been obvious to a person of ordinary skill in the art upon a reading of Lewis and Jordan, either separately or in combination. Thus, it is believed that claims 1, 7-8 and 13 are allowable under 35 U.S.C. §103. Withdrawal of this rejection is respectfully requested.

Rejection of Claims 3-4, 9 and 14 under 35 U.S.C. §103

Claims 3-4, 9, and 14 stand rejected under 35 U.S.C. §103 as being unpatentable over Lewis and Jordan in view of Loc. This rejection is respectfully traversed.

Claims 3-4 and 14 depend ultimately from independent base claim 1, and claim 9 depends from independent base claim 8.

The patentability of the base independent claims has already been discussed above and will be understood to be incorporated herein without further repetition, except to repeat that the combination of Lewis and Jordan fails to teach, show, or suggest all the elements of the base independent claims. Loc was introduced because it was stated that the combination of Lewis and Jordan failed to disclose the operation of an encryption failure counter, whether incrementing or resetting to zero. Since there is no additional showing that Loc cures the deficiencies of Lewis and Jordan as described above, it is submitted that the combination of Lewis, Jordan, and Loc fails to disclose or suggest all of the elements of claims 3-4, 9 and 14.

In light of the remarks above and because of the dependence on the independent base claims discussed above, it is believed that dependent claims 3-4, 9 and 14 would not have been obvious to a person of ordinary skill in the art upon a reading of Jordan, Lewis, and Loc, either separately or in combination. Thus, it is submitted that claims 3-4, 9 and 14 are allowable under 35 U.S.C. §103. Withdrawal of this rejection is respectfully requested.

Rejection of Claims 5-6 and 10-12 under 35 U.S.C. §103

Claims 5-6 and 10-12 stand rejected under 35 U.S.C. §103 as being unpatentable over Lewis and Jordan in view of Kelem. This rejection is respectfully traversed.

Claims 5 and 6 depend ultimately from independent base claim 1, and claims 10-12 depend from independent base claim 8.

The patentability of the base independent claims has already been discussed above and will be understood to be incorporated herein without further repetition, except to repeat that the combination of Lewis and Jordan fails to teach, show, or suggest all the elements of the base independent claims. Kelem was introduced because it was stated that the combination of Lewis and Jordan failed to disclose setting the encryption key to a null value. Since there is no additional showing that Kelem cures the deficiencies of Lewis and Jordan as described above, it is submitted that the combination of Lewis, Jordan, and Kelem fails to disclose or suggest all of the elements of claims 5-6 and 10-12.

In light of the remarks above and because of the dependence on the independent base claims discussed above, it is believed that dependent claims 5-6 and 10-12 would not have been obvious to a person of ordinary skill in the art upon a reading of Jordan, Lewis, and Kelem, either separately or in combination. Thus, it is submitted that claims 5-6 and 10-12 are allowable under 35 U.S.C. §103. Withdrawal of this rejection is respectfully requested.

Conclusion

In view of the foregoing, it is respectfully submitted that all the claims pending in this patent application are in condition for allowance. Entry of this amendment, reconsideration, and allowance of all the claims are respectfully solicited.

If, however, the Examiner believes that there are any unresolved issues requiring adverse final action in any of the claims now pending in the application, it is requested that the Examiner contact the Applicants' attorney at 609-734-6834, so that a mutually convenient date and time for a telephonic interview may be scheduled for resolving such issues as expeditiously as possible.

Respectfully submitted,

August 17, 2009
Date

/Wan Yee Cheung/
Wan Yee Cheung
Attorney for Applicants
Registration No. 42,410

U.S. Patent Operations
Thomson Licensing Inc.
P.O. Box 5312
Princeton, NJ 08543-5312
Phone: 609-734-6834